

DSS:AAS  
F.#2012R00502

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

M -0315

- - - - - X  
UNITED STATES OF AMERICA

- against -

TO BE FILED UNDER SEAL

THE PREMISES KNOWN AND DESCRIBED AS  
1685 GRAND AVENUE, SUITE 205,  
BALDWIN, NEW YORK

AFFIDAVIT IN SUPPORT OF  
SEARCH AND ARREST WARRANTS

(T. 18, U.S.C., § 1349;  
Fed. R. Crim. P. 41)

- - - - - X  
- - - - - X  
UNITED STATES OF AMERICA

- against -

CARL O. BENNETT,

Defendant.

- - - - - X

EASTERN DISTRICT OF NEW YORK, SS:

BRYAN J. TREBELHORN, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS 1685 GRAND AVENUE, SUITE 205, BALDWIN, NEW YORK (the "SUBJECT PREMISES"), located within the Eastern District of New York and further described below, the things described in Attachment A, all of which constitute evidence, fruits and instrumentalities of

violations of Title 18, United States Code, Sections 1343, 1344 and 1349 (bank fraud, wire fraud, and conspiracy to commit bank fraud and wire fraud).

Upon information and belief, on or about and between January 1, 2001 and March 20, 2012, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant CARL O. BENNETT, together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud financial institutions, and to obtain moneys, funds, credits, assets, securities, or other property, owned by and under the custody and control of such financial institutions, by means of materially false and fraudulent pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Section 1349)

The source of your deponent's information and the grounds for his belief are as follows:<sup>1</sup>

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal

---

<sup>1</sup> Because this affidavit is submitted for the limited purpose of establishing probable cause for search and arrest warrants, I have not set forth each and every fact learned during the course of the investigation.

laws and duly authorized by the Attorney General to request a search warrant.

2. I have been a Special Agent with the FBI for approximately four years, and I am currently assigned to a financial institutions fraud squad, which investigates violations of federal criminal laws affecting financial institutions and other financial crimes. In this position, I have conducted physical surveillance, interviewed witnesses, reviewed extensive documents obtained through the service of subpoenas, and used other investigative techniques, including execution of search warrants, to secure relevant information for use in criminal prosecutions.

3. My knowledge of the information set forth in this affidavit is based upon my personal participation in this investigation and in numerous other investigations of fraud perpetrated against financial institutions, including bank and wire fraud, my review of records and reports, my debriefing of cooperating witnesses, my discussions with witnesses and victims, my conversations with other law enforcement agents involved in this investigation and similar investigations, my conversations with and review of information provided by financial institutions, and my law enforcement experience and training.

4. I have personally participated in the investigation of the offenses discussed below. I am familiar

with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, and (c) information obtained from confidential sources of information.

I. DESCRIPTION OF THE SUBJECT PREMISES

5. The SUBJECT PREMISES is an office space located inside a commercial building located on the east side of Grand Avenue, between Stanton Avenue (to the north) and Stowe Avenue (to the south) in Baldwin, New York. The front entrance to the building consists of a single glass door. Located above the glass door, in white lettering is the number "1685." Behind the front entrance, there is a lobby with an elevator on the northeast side of the lobby and a two-level staircase located on the northwest side of the lobby. The SUBJECT PREMISES is located on the second floor of this commercial building, behind a green door marked by a gold plate with the number "205" in black lettering.

6. A confidential source, who has previously provided reliable information as described below, has informed law enforcement agents that the SUBJECT PREMISES consists of an office room containing a desk facing a wall and three computer towers, as well as a file storage room.

II. PROBABLE CAUSE AS TO THE SUBJECT PREMISES  
AND THE ARREST WARRANT

A. Introduction

7. Since 2001, a group of co-conspirators have defrauded various lending institutions (the "Lenders") by obtaining mortgages on properties (the "Properties") located in the Eastern District of New York and elsewhere through fraudulent means, including by falsifying mortgage loan applications, appraisals, title reports, bank records, employment records, and other documents. That false information made the borrowers appear to be more creditworthy, and falsely enhanced the purported value of the Properties. As a result, the Lenders were fraudulently induced to issue mortgage loans secured by the Properties.

8. The co-conspirators recruited purchasers (the "Purchasers") who desired to purchase the Properties for their own use. The Purchasers generally were individuals with good credit scores, but with income and assets that were insufficient to secure a mortgage loan. The co-conspirators often promised the Purchasers either that no down payment would be necessary to purchase the Properties, or that any down payment would be refunded to them at the closings.

9. The co-conspirators also recruited Straw Buyers to pose as the purchasers of some of the Properties. Like the Purchasers, the Straw Buyers generally were individuals with good

credit scores, but with income and assets that were insufficient to secure a mortgage loan. Unlike the Purchasers, however, the Straw Buyers did not intend to inhabit or control the Properties. Instead, the co-conspirators were the true owners of the Properties purportedly purchased by the Straw Buyers. In exchange for the use of their names and good credit, the Straw Buyers often received a fee.

B. The Fraudulent Scheme

10. Once Purchasers or Straw Buyers were recruited, the co-conspirators prepared and caused to be prepared mortgage applications for the Properties. These mortgage applications contained numerous misrepresentations and material falsehoods designed to make the Purchasers and Straw Buyers appear more creditworthy. Among other things, the mortgage applications falsely inflated the bank account balances and income for the Purchasers and Straw Buyers. Additionally, some of the mortgage applications falsely stated that the mortgage applicants would live at the Properties. The co-conspirators caused these applications and supporting documents to be sent to the Lenders by facsimile or via electronic transmissions.

11. As a condition for issuing the mortgage loans, the Lenders required the Purchasers and Straw Buyers to make down payments on the purchase of the Properties. Notwithstanding

these requirements, the Purchasers and Straw Buyers often did not make any down payments.

12. In many instances, the Purchasers and Straw Buyers failed to make mortgage payments to the Lenders, and the mortgage loans for the Properties defaulted.

B. The Defendant

13. Since approximately 1988, the defendant CARL O. BENNETT has owned and operated COBacts, Inc., which is a financial services company that provides tax preparation, investment, and travel services. The investigation has revealed that, on numerous occasions, BENNETT conspired to obtain mortgage loans from Lenders through fraudulent means. Specifically, BENNETT created fraudulent financial documents to be submitted to the Lenders together with mortgage applications.

C. The Defendant's Creation of Fraudulent Documents at the SUBJECT PREMISES

14. The government has indicted and arrested a co-conspirator in the mortgage fraud scheme described above, on charges of bank and wire fraud conspiracy. Since his/her arrest, the co-conspirator (hereinafter the "CS") has cooperated with law enforcement authorities.<sup>2</sup> In post-arrest debriefings, the CS informed the government that, prior to the CS's arrest and on

---

<sup>2</sup> The CS faces a significant term of incarceration for CS's role in the mortgage fraud. The CS has provided the information described herein in the hopes of obtaining a reduced sentence. To date, CS's information has proved reliable.

numerous occasions, the CS and other co-conspirators had purchased pay stubs and IRS Forms W-2 from the defendant CARL O. BENNETT for submission to the Lenders in connection with fraudulent loan applications.

15. In early December 2011, while acting under agent supervision, the CS visited the defendant CARL O. BENNETT at the SUBJECT PREMISES. The CS was equipped with a recording device.

16. During the meeting, the CS informed the defendant CARL O. BENNETT that the CS needed falsified documentation for a Purchaser seeking a mortgage loan from a Lender ("Purchaser-1"). The CS told BENNETT that Purchaser-1 earned approximately \$36,700 but needed documentation to reflect that Purchaser-1 earned approximately \$56,720 per year. The CS provided BENNETT with Purchaser-1's actual Forms W-2. BENNETT agreed to create false pay stubs and Forms W-2 for Purchaser-1 by using "ADP pay stubs." BENNETT informed the CS that he would charge \$400 for the pay stubs and Forms W-2. BENNETT also informed the CS that he could create false bank statements by scanning actual bank statements onto his computer and making changes to the scanned documents. BENNETT asked the CS to obtain a printed copy of Purchaser-1's bank account statement for BENNETT to alter.



17. On approximately March 20, 2012, while acting under agent supervision, the CS visited the defendant CARL O. BENNETT at the SUBJECT PREMISES again. The meeting was recorded on audio and videotape. During the meeting, BENNETT described how he typically creates fraudulent ADP pay stubs and how he determines what deductions should be reflected on the false pay stubs. In particular, BENNETT stated that he does not use false dependents on the fabricated pay stubs. The CS provided BENNETT with \$400 and stated, "I have the pay stubs. Give me the W-2s." BENNETT provided the CS with fraudulent Forms W-2 for Purchaser-1 and stated, "These are the W-2s." BENNETT added that the Forms W-2 that he had created were "9 and 10," referring to years 2009 and 2010. The CS informed BENNETT that the CS may be asked for year 2011 Forms W-2, as well as two pay stubs. BENNETT responded that he had these documents on his computer and that he would have to update them for 2011, as the format for ADP Forms W-2 had recently changed. After making changes to the documents on a computer in the SUBJECT PREMISES, BENNETT provided fraudulent Forms W-2 for Purchaser-1 to the CS.

18. During the same conversation, the defendant CARL O. BENNETT described how he stored important files on a portable UBS drive, which he referred to as his "jumpjack" (hereinafter the "Jumpjack"). BENNETT showed the Jumpjack to the CS. BENNETT stated that, whenever he leaves the SUBJECT PREMISES

for an extended period of time, he takes the Jumpjack with him. BENNETT described the Jumpjack as "the most important thing in the office."

19. Also during the meeting, the defendant CARL O. BENNETT described services he rendered to other clients. For example, BENNETT stated, "I did bank statements, I did a whole bunch of stuff: pay stubs, W-2s, tax returns." Showing the CS one of BENNETT's work computers, BENNETT also showed the CS different formats used to create false documents. With respect to creating fraudulent bank records, BENNETT stated, "Chase I do, not Citibank." Video footage from meeting shows a computer screen with a scanned image of a Capital One check. At the conclusion of the meeting, BENNETT instructed the CS, "[D]on't disappear from me."

### III. Scope of the Proposed Search

20. I have been informed by Assistant U.S. Attorney Alexander A. Solomon that, under the relevant case law, in the event of a search of business premises that are "permeated with fraud," a broad search warrant that authorizes the search and seizure of voluminous business records does not run afoul of the Fourth Amendment. National City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980) (citing United States v. Brien, 617 F.2d 299, 309 (1st Cir. 1980)); see also United States v. Johnson, 108 F.3d 1370, 1997 WL 136332, at \*3 (2d Cir.

Mar. 21, 1997) (unpublished summary order) (affirming broad search where affidavit "show[ed] ample ground for finding pervasive fraud"). In this case, given the long time period that the defendant CARL O. BENNETT has participated in the mortgage fraud conspiracy, a broad seizure of business records, including computerized records, from the SUBJECT PREMISES is warranted.

21. Based upon the information set forth and incorporated above, my training, experience, and participation in this and other financial crime investigations, and my conversations with other law enforcement officers, there is probable cause to believe that the SUBJECT PREMISES is being used by the defendant CARL O. BENNETT for the storage of various financial records and documents relating to bank fraud and wire fraud and conspiracy to commit bank fraud and wire fraud.

22. Based upon the information set forth and incorporated above, my training, experience, and participation in this and other financial crime, and my conversations with other law enforcement officers experienced in investigations of similar crimes, I know that persons who commit frauds such as this one often maintain records relating to the fraud in secure locations to which they have ready access, including their places of business. More specifically, I know that persons who commit frauds such as this one are apt to maintain records such as:

- a. Documents<sup>3</sup> relating to the finances of persons or entities perpetrating the fraud, as well as bank account information and records, including loan records, that identify victims of fraudulent schemes, participants in fraudulent schemes, and loss amounts;
- b. Documents relating to assets, liabilities, income, expenses, sales and accounts receivable, such as accounting records, invoices, and federal and state tax records (including income tax records);
- c. Documents relating to any mail box located at a commercial mail receiving agency, including customer applications and correspondence;

---

<sup>3</sup> The term "document" is used in this paragraph and all its sub-paragraphs in the broadest sense and includes, without limitation, any written, graphic, or recorded matter, however produced or reproduced, any drafts thereof, any marginal notes or comments appearing on any document, and each and every tangible thing from which information can be processed or transcribed, such as tape, microfiche, microfilm, CD-ROMs, DVDs, hard drives, servers, cassettes, cartridges, digital cameras, cellular phones, personal digital assistants (PDAs) and memory cards or other electronic data communications, and copies of documents which are not identical duplications of the originals (e.g., because handwritten or blind copy notes appear thereon or are attached thereto).

- d. Documents relating to communications or contacts between the co-conspirators and any of their principals, employees, agents, or victims; and
- e. Documents relating to the co-conspirators', or any of their principals', employees', or agents' calendar, contact, or personal planner data or files.

23. Based on all of the foregoing information, my training and experience in law enforcement, my involvement in fraud investigations, my participation in the execution of numerous search warrants in connection with those investigations, and my conversations with other law enforcement officers experienced in investigations of similar crimes, I conclude that there is probable cause to believe that there is presently located within the SUBJECT PREMISES evidence and instrumentalities, as set forth in Exhibit A, of violations of federal law, including violations of 18 U.S.C. §§ 1343, 1344 and 1349.

#### IV. STORING AND SEARCHING ELECTRONIC MEDIA

24. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including

hard disk drives, floppy disks, compact disks, magnetic tapes, memory chips and other portable and removable media. I also know that during the search of a building it is not always possible to search computer equipment and storage devices for data. I and other federal law enforcement officers will make every effort to "image" or copy original computer servers in such a way that we will not have to seize them, but such a procedure may not be possible in this case for a number of reasons, including the following:

25. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data, or even just image it, during the execution of the physical search of a building. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing at least 160 gigabytes ("GB") of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.

26. Searching computer systems is a highly technical process which requires specific expertise and

specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

27. Because voluminous amounts of information can be stored in a computer or electronic storage devices (such as hard disks, USB "flash" drives, diskettes, tapes, laser disks, and magneto opticals), and because information might be stored in a deceptive fashion or with deceptive file names to conceal criminal activity, the searching authorities must carefully open and examine all the stored data to determine which of the various files are evidence, fruits, or instrumentalities of the crime. This sorting process can take days or weeks, depending on the volume of data stored, and would be impractical to do on site.

28. This sorting process is highly technical and requires expert skill and, on occasion, specialized equipment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. Similarly, it is difficult for the expert to know before a search what computer

hardware and software might be necessary for him or her to analyze the data and to recover potentially "hidden," erased, compressed, password-protected, or encrypted files.

29. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to ensure the integrity of the data recovered and reduce the possibility of inadvertent modification of the data in question.

30. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is



concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

31. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to

retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

32. I and other federal law enforcement officers will make every effort to "image" or copy original computer servers from the SUBJECT PREMISES in such a way that we will not have to seize them, but, for the reasons outlined above, I request authority to search, copy, image and seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the image or hardware for the evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 1343, 1344, and 1349.

V. SEARCH METHODOLOGY TO BE EMPLOYED

33. The search procedure of electronic data contained in computer hardware, computer software, and/or electronic storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls

within the items to be seized as set forth herein;


- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear

in the evidence described in Exhibit A;  
and/or

- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described on Exhibit A.

WHEREFORE, your deponent respectfully requests that a search warrant issue, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, allowing Special Agents of the Federal Bureau of Investigation and other federal agents, with proper assistance from other law enforcement officers, to search, gain access to, and retrieve from the SUBJECT PREMISES, the items set forth in Attachment A, whether in document form or stored on any electronic, optical, magnetic or computer media, that constitute or show evidence and instrumentalities of 18 U.S.C. §§ 1343, 1344 and 1349.

WHEREFORE, your deponent also respectfully requests that a warrant issue for the defendant CARL O. BENNETT so that he may be dealt with according to law.

  
BRYAN J. TREBELHORN  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
21th day of March, 2012

1  
1  
1

U